THE PROBLEMS OF IMPLEMENTING ELECTRONIC SIGNATURES IN A WIRELESS ENVIRONMENT

Raj GURURAJAN

Department of Information Systems, University of Southern Queensland,
Toowoomba, QLD 4350

ABSTRACT

The topic of wireless devices[1] is now high on the policy of many countries that have revisited their regulatory framework because these devices support electronic transactions. Despite the advancements in the legal system to address a number of issues influencing transactions arising out of these mobile devices, it appears that organizations are yet to comprehend the full impact of these legislative procedures as these procedures include technical as well as management components. When organizations perform electronic transactions using wireless devices, the concept of electronic signatures becomes an integral part of transactions negotiated. Depending upon the context, the enforcement of many issues with respect to this electronic signature vary. For instance, while it is perfectly valid to attach an electronic signature to a simple purchase of a book, it may not be possible to attach the signature to a property deal as regulatory framework in certain countries do not accept electronic forms of signatures for property transactions. While the electronic signature helps to identify a person who has involved in a transaction electronically, due to various technical issues associated with wireless devices, it is difficult to interpret who the sender is, how to authenticate the signature, how the data message is transmitted, and the validity of enforceable issues.

This paper investigates aspects of United Nation's Model Law with specific focus to 'signature' elements. The discussion provided in this paper also highlights the impact of electronic signatures on organizations that use wireless devices for the purpose of electronic transactions.

KEYWORDS: Electronic Signatures, Wireless Technology, Legal Issues

INTRODUCTION

Due to technological advancements, 'Globalization' has become a paradigm in today's business world. Introduction of mobile devices such as mobile phones has definitely encouraged lots of small businesses to embrace globalization without being bogged down by traditional organizational infrastructure associated with resources. The mobility offered by electronic devices such as PDAs has encouraged businesses to deal with customers at anytime, anywhere and anyhow. The 'anyhow' component is new, facilitated by the mobile devices and distinct from the Internet model. The mobility of devices not only facilitates business transactions but also 'localize' certain components based on the location of the user.

In order to support business transactions arising from wireless devices, there has to be some kind of harmony between trading partners in terms of regulations, as the

[1] The term 'wireless devices' is used interchangeably with 'mobile devices' in this paper.

transaction may pass through a number of intermediate agencies residing over many countries. For example, a transaction in a mobile commerce typically involves a buyer, seller, a financial institution and a delivery agency. Therefore, if harmony is not found, especially in digital communication channels, businesses may find it difficult to realize and fulfill a transaction. Hence, the United Nations created a set of laws, called UNCITRAL "Model Law" to facilitate electronic transactions. Due to the rapid growth of e- and m-commerce activities, these laws were revised to incorporate a number of new amendments in order to facilitate electronic transactions. Among these, the electronic transaction laws are important because these laws address issues relating to digital transactions.

It appears that businesses involved in international transactions are not conversant with the recent changes to the digital signature regulations. Any relative ignorance in the area of electronic signatures and the associated issues will lead into potential problems when trading in international domains. The purpose of this paper is to provide an overview of different regulations governing digital signatures and how these regulations influence businesses conducting transactions using wireless devices. This paper will also highlight some glaring overlaps and confusions in interpreting or reading the digital signature regulations.

IDEA BEHIND ELECTRONIC SIGNATURES

The concept of signature is not new and is in existence for several hundred years. When a document is "signed", the signature serves a number of purposes. The signature identifies a person; it provides certainty as to the personal involvement of that person in the act of signing; it associates a person with the content of a document; it might attest to the intent of a party to be bound by the content of a signed contract; it might endorse the intent of a person to certify the authorship of a text; it might endorse the intent of a person to associate with the content of a document written by someone else; it might reveal details such as time and date of the correspondence. Signatures also play a vital role in identifying characteristics of a document as well as the person originating the document (Clarke, 2003).

It is worth noting that in addition to written signatures, a number of other forms of signatures are also available. These are stamps, perforation, etc. The purpose of these signatures is to provide various levels of certainty. For example, in some countries, there exists a general requirement that contracts for the sale of goods above a certain amount should be signed on a statutory document in order to be enforceable. In addition to these forms, there are occasions when these forms of signatures need to be witnessed by neutral bodies and the evidence of such witness is provided by traditional handwritten signatures. In essence signatures satisfy the authentication requirements for a document (Stowe, 2000).

Electronic signatures are realized when the functions of traditional signatures are transformed into an electronic form. It should be noted that the 'functions' of signatures should be transformed and not a mere electronic copy of a signature. Therefore, the term electronic signature refers to certain functional aspects of a traditional signature and NOT a scanned form of a signature. The main purpose of electronic signatures is to provide reliability and security to electronically transmitted messages. The security and reliability are provided by mechanisms to create an electronic tag that is annexed to the message (McCullagh, Little, & Caelli, 1998).

This tag is unique and can't be reproduced by unauthorized people. In simple terms, theoretically, these electronic signatures can't be forged.

Electronic signatures are usually a means of identification of a person and of the intent of that person to be associated with that electronic record. The term record refers to a transaction, a contract, a letter or any other form of communication. In modern day transactions, these may include communication established via emails as emails constitute a written document. It is important to note that the term electronic signature has no universally accepted meaning and is variously defined in different statutes (Judge, 1998). The technology that helps to realize an electronic signature is called encryption technology, which uses 'electronic keys' or to lock and open messages.

In the domain of electronic transactions, a range of electronic authentication methods – of varying security and reliability – is available for a person to authenticate an electronic record. The authentication can include typing a name at the end of an email, a personal identification number and the swiping of a magnetic card, typing passwords, transmitting a digitized version of a manual signature, encryption of a message using a key and biometric forms (Sneddon, 1998). While all these methods can be interpreted as a form of electronic signatures, for the purpose of business oriented transactions, electronic signatures refer to an electronic tag that is found in a message transmission to identify the originator of the transaction.

WHAT IS AN ELECTRONIC SIGNATURE ACCORDING TO THE UNCITRAL MODEL LAW?

Article 7 of Model Law developed by the United Nations (UN) addresses a number of issues associated with electronic signatures. This article focuses on two basic functions of electronic signatures. The first function is to identify the author of the document and the second function is that the author approved the content of the document.

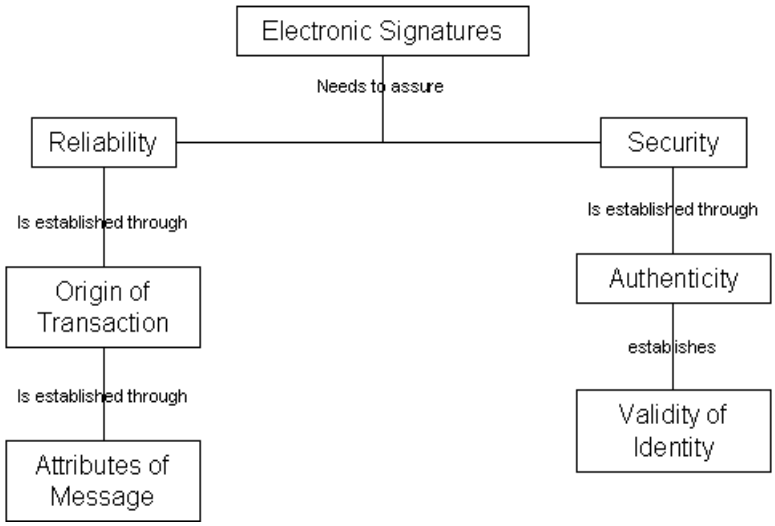
The first section (denoted as (1) in the article) of the article identifies two specific functional elements of an electronic signature. They are the **method** (specified in 1(a)) and **approach** (specified in 1(b)) through which the method is established. The article very clearly specifies that the method used under paragraph 1(a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all circumstances, including any agreement between the originator and the addressee of the data message.

Further, the article states that "… (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature".

This statement is crucial to business transactions using wireless devices because businesses need to fulfill certain obligatory requirements to its consumers, in addition to follow the law. When it comes to law, the concept of evidence assumes importance and businesses need to produce various evidence to justify any claims that they are making in resolving disputes between various elements involved in a transaction.

While Article 7 stipulates the concept of 'signature', it is not clear as to how to enforce this concept when things go wrong. Further, the article was written when the desktop computers were predominantly available and most of the functions facilitated by desktop computers have been built into mobile devices. Due to the mobility of these devices, the concept of 'signature' becomes complicated and hence the interpretation. For example, when users with mobile devices 'roam', the service providers of foreign networks may not support certain services prescribed by these users. So, any assumption made by the users regarding the service level agreements may fail.

According to Article 7, when a transaction is conducted over a communication medium, such as the Internet, businesses need to ensure and satisfy that the transaction is reliable and secure. The reliability is established in terms of the origin of the transaction, receipt of the transaction message, and the integrity of the information transmitted. This is shown in the following diagram. The security is established in terms of authenticity.



In addition to this, the identification of parties involved is also essential in electronic transactions. The clarity of contents is most crucial to understand subject matter. If the contents contain of garbage characters, then understanding of the information is a problem (Wyrough & Klien, 1998). While regulations stipulate a number of issues associated with an electronic transmission, the legibility of messages (in a wired environment) are left out as this can't be guaranteed by communication providers. In the case of wireless devices, this becomes a crucial issue as external interferences can affect the quality of communication and the service providers may not be able to undertake any responsibility for the poor quality. One example is the 'weather' conditions such as storms that can affect wireless quality. Currently, there is no protection for businesses as well as consumers.

Security is established in terms of authenticity of the message, whether the person whose name is the bearer, is actually the person and whether the message can be reproduced or duplicated by unauthorized users. Electronic technologies such as transmission protocols, encryption are used to ensure the reliability and security of the message (Kuechler & Grupe, 2003; Clarke, 2003). While the technologies exist for

providing security to users, device manufacturers have deliberately ignored to provide high level security features on wireless devices due to memory and other hardware restrictions. Therefore, the implementation of security is left with users at their own cost. Usually this is done through service providers at an additional cost.

Authentication, a component of electronic signature, is generally defined to establish the validity of the identity of a particular entity in a transaction. This entity could be a sender or a receiver. Electronic signatures serve the purpose of verifying the authenticity of the parties involved. To achieve this, electronic signatures use the cryptic technology to transform the transaction in a form that is not easily understood (Evans, 2000). This technology uses a pair of keys to crypt the messages. The keys are usually stored on the computer hard disks. When this is implemented on wireless devices, when the devices are lost, the keys are also lost and subject to unauthorized use.

LEGAL CONSEQUENCES ARISING WHILE IMPLEMENTING ELECTRONIC SIGNATURES

When businesses trade in international domain, they should be aware of various legal issues binding the concept of signature and the undecided issues influencing electronic signatures. For example, the question that '*Can we accept electronic signature as a signature?'* is not yet fully and satisfactorily answered.

It has already been mentioned that a signature is only an authentication. In other words, signature serves the purpose of a mark. The legal requirement is that the mark be made by the person on the document or by authority in order to satisfy legal requirements. When the signature is not needed to be an autograph, then a printed name is enough to satisfy the legal requirements. In certain cases, stamps can be used to satisfy legal requirements. In certain specific cases, the stamp is supported by the signature of the person.

There are three important points to note here (Lovell, 2000). In a traditional setting where paper is the medium,

1. to constitute validity of a person's signature, there is no need that the person should be physically act by putting signature on the document. For example, this can be achieved via an agent. In some cases, a power of attorney can be given to specific parties to achieve this purpose.

2. the signature alone assures the authenticity of the genuineness of a document in most cases. If this is not sufficient, other forms of signatures such as a stamp or watermark can accompany the signature to assure the authenticity.

3. the person must put his or her mind to the act of signing the document in order to be bound. This act is applicable for the signatory as well as the witnesses. Compulsion does not form the component of act and hence it may not be possible to bind the person and his signature.

When we apply these three points onto a wireless domain, certain legal complication arise at the time of implementation. For example, a wireless device such as a mobile telephone is conceived to be a person's identity because the device is sold to a person

or an organization and a unique number is allocated to that device. Therefore, the concept of electronic signatures may become valid at this point and any transactions originating from this device can be accepted. When such a transaction is generated, the device identification, in this case, a mobile telephone number, forms a part of signature. However, when the device is used by another person to conduct a transaction, can it be safe to assume that the telephone number alone is sufficient to establish 'signature'? While it is possible to ensure the concept of signatures in a wired environment, it may not be always possible to ensure the same in a wireless environment. Further, as the wireless devices pass through various networks or cells, the quality of services provided to users may not be uniform and hence the composition of signature may suffer.

In a traditional setting, the authenticity of a document can be guaranteed in many ways. For instance, an original can be distinguished from a forged document using certain simple checks. When it comes to wireless devices, this may not be possible. For instance, certain cellular networks may not display the mobile numbers of other network users, resulting in the identity being not revealed. When calls are made from organizational extension, in many cases, only the main switch board number is provided to the network providers and not the extension, resulting in identity not disclosed. Therefore, there is a problem in establishing the identity of the person conducting the transaction and hence the question of authenticity of such a transaction. Further, it should be noted that the cryptography technique is well developed in the area of text messages. When it comes to voice based transactions, the techniques are not so well developed and hence the authenticity of such transactions is not reliable.

While, the current technology can perhaps assure the first two points above, the third point is complicated. Due to the relative distances involved how to guarantee that a person has 'signed' a document without any external influences at the time of signing? For instance, let us assume that a transaction is performed using the keypad of a mobile device such as mobile telephone or a PDA. It may be possible to respond to a string of questions using the keys available on the keypad of these devices. A person can be forced to use these keys by force. As there may not be any witnesses, how is it possible for a person negotiating at the other end to recognize these contexts? Therefore, it is difficult to accept electronic signatures comparable to traditional signatures in these circumstances.

Some further argument is provided below to highlight how the concept of electronic signatures is difficult to implement in a wireless world.

When electronic documents are sent through wireless devices, two specific scenarios can happen:

1. It may be possible for an anonymous person to access wireless messages using some sniffing software applications in an unauthorized manner. For instance, when person A is operating a mobile phone, the messages can be intercepted by person B without person A's knowledge.

2. The mobile device can be stolen by person B. Then person B can impersonate person A to establish communication using the stolen device. This can fall under the case of 'identification theft', where a person can pretend to the

owner of the instrument. This can lead to electronic fraud similar to credit card frauds. In some countries, the concept of a 'virtual credit card' is trialed. The concept involves developing a credit card that can be displayed on the mobile phone display screen. When the instruments are stolen, the credit card is also stolen, leading to financial fraud.

3. In addition to this, it is possible for the document to be captured while in transmission, modified without the knowledge of the sender. This may by mistake bind the sender to the contents of the document. In this case, the electronic signature cannot be accepted equivalent to the traditional signature. This is because, in traditional media, any modification can be detected and hence the concept of signature is valid in traditional media.

4. Further, as mentioned earlier, while conducting electronic transactions using mobile devices, usually keys available on the keypad of the devices are used to verify identity. Examples of this verification include Personal Identification Number (PIN). What is lacking in this system is establishing identity beyond doubt as PINs can be stolen. Therefore, the concept of signature may not hold well in this instance.

Therefore, the concept of signature can't be accepted always in a wireless environment.

Another question that hasn't been answered is *'What happens when there is a fraud – Can we accept electronic signatures?'* According to McCullagh et al, there is widespread support to establish that in cases of frauds, electronic signatures can be used to establish the integrity. It has been suggested that a signature to be valid under the Statute of Frauds must specify the name of the person to be bound. It has been clearly specified that a mark (such as a company stamp) that doesn't specify the person's name is insufficient. Then the question that a mark that does not directly specify the signer's name but can be indirectly linked to he relevant person, will suffice can arise. In electronic signatures, it is possible to use the concept of a certifier to certify the signatures. This electronic certificate will be able to specify the name of the signer of the message. This indirect access to the name of the signatory should satisfy the Statute of Frauds, provided the integrity of the electronic certificate is assured. The electronic certificate should be able to identify the signer despite the fact that the identification process does not arise from the document itself but arises through some indirect secure method (Stowe, 2000). While the concept of certification is prevalent in wired environment, in wireless environment this concept is still in its infancy stages. Many wireless device manufacturers and software developers are still in the process of developing cost effective applications to address this issue and hence, in the current context, the certification of signatures is not available.

When it comes to disputes, in many cases, the legal system demands evidence. In many contractual obligations such as sale of property, witnesses are engaged to ascertain to guarantee the legitimacy of signatures. When it comes to the wireless domain, '*The validity of the role of witnesses*' is yet to be answered satisfactorily. The argument for this is provided below.

In traditional systems, a witness will be able to read the document and then sign the document. In certain cases, the witness will be able to attest a document to guarantee that the person who signs the documents is the person in question. In other circumstances, notary public and authorized officials will be able carry out these duties. The purpose of witness is to avoid any potential forgery. The role of witness is crucial in documents such as deeds (McCullagh et al., 1998). When a dispute arises, usually the document in question is put before a court along with the witnesses. The court will inspect the document and cross-examine the witnesses in the process of settling the dispute. Witnesses are usually aware this procedure.

In the case of traditional transactions, witnesses sign the document on their own. The act of signing or stamping is conducted according to their will and they engage themselves with complete knowledge in doing so. The signing is to endorse the person who is going to be bound by the document and NOT to endorse the contents of the document.

This raises an interesting question. Is it possible for an attester to witness an electronic signature? In the traditional process, a witness understands the concept of writing and the concept of stamps. The process of well understood and in existence for centuries. When the same process is conducted using an electronic media, the process need not have to be straightforward. What the computer screen displays and what is actually retained in computer memory may be two different things. Further, the execution of certain keystrokes may be beyond the comprehension of the attester and these keystrokes can generate the electronic signatures. The witness may not understand the process of generating electronic signatures and associated security issues in order to ensure that the electronic signatures refer to the person who is actually initiating them. The keystrokes involved will not reveal the true processing sequences in generating the electronic signatures. Therefore, it can be said that the witnesses do not engage themselves fully in the operation. This area needs more discussion in terms of legal consequences and technical development (McCullagh et al., 1998).

It should be noted that the current regulations do not provide any solution to this problem.

WHAT ARE THE DUTIES OF A SIGNATURE HOLDER AND THE CONSEQUENCES OF A BREACH OF THESE DUTIES

It is generally agreed that a signature holder will have a duty of care to avoid the unauthorized use of his or her signature. Further a signature holder will also prevent the recipient from relying on an unauthorized use of his or her signature. However, there is no consensus on the consequences, which are to follow from a breach of this duty of care, or even whether such a statement of the duty of care needs to be contained in the Uniform Rules. In certain countries, the legal system stipulates that the signature holder is responsible for the consequences of breaching these obligations, but leave it to each State's national law to determine the nature of those consequences. An alternative provided by some countries include that regulatory authorities should specifically set out the consequences of breaching those obligations if they are to foster the development of harmonized rules on electronic signatures. To understand this issue, we need to read beyond Article 7. Some information is contained in Article 13 of the UNCITRAL Model Law, which is beyond the scope of

this paper. One clear problem with specifying the consequences of breaching the obligation is considering how a provision like draft article 7, which establishes a liability rule for the attribution of a signature, relates to article 13 of the Model Law on the attribution of a data message. It will be important to avoid confusion, in cases of signed data messages, as to which provision should be used to attribute the data message and deal with liability. When it comes to wireless domain, not only the data message (written) is applicable, but also data message (spoken) is applicable as well. Therefore, further consideration is needed here to distinguish between these two types of data messages in order to establish the concept of signature.

LEGAL ISSUES

One of the principal legal issues that warrant careful consideration is the task of adapting existing legal and evidentiary requirements to the new means of contracting and communicating using wireless devices. Due to the number of intermediaries playing an active role in completing a transaction, it is essential to establish and determine the place and time of the contract in resolving disputes. When a contract is drawn using the traditional processes, the place and time stamps are automatically recognized. In addition to these stamps, a notary public will be able to authenticate the parties involved. However, when it comes to online contracts originating from mobile devices, these procedures may not be applicable (Desai, 1999).

Businesses face a major problem here. For example, when an insurance policy is taken by a business, the insurance intermediary's computer can automatically generate an acceptance of customer details and can generate a cover note. This cover note then can be sent to the customer. In this process, there is no human intervention. What happens if the computer generates some garbled message? *Who is responsible* for such garbled messages? Who is bound by these messages? Who is responsible (sender, ISP or another body involved in transmission) for errors generated in the overall processes? The transactions act does not control this.

The second problem that faces the businesses is the *issues of proof*. In an electronic transaction, such as the one mentioned above, how can one establish the identity of the offeror and offeree? What happens when a person other than the owner or authority of the device sends an electronic message causing damages? The transactions act does not stipulate this clearly.

How can businesses reduce the legal risks when trading using wireless technology? Businesses should be aware of various legal issues in the area of contracts, how they are developed and generated, what are the binding agreements, the concept of authenticating parties signing the contracts and other international regulatory issues.

CONCLUSION

Despite the technical development in the domain of wireless technology and despite the recent changes to the regulatory framework, it appears that there are difficulties in fully understanding and implementing the concept of electronic signatures on wireless devices. When businesses deal in a global environment, electronic signatures pose a problem at the time of enforcement. Due to certain domestic understanding of the concept of signatures, the implementations of electronic signatures vary between countries. While national laws attempt to address the problems in their jurisdiction,

businesses may find it impossible to apply the national regulatory framework to international disputes.

The United Nation's Model Law provides some form of solutions by recognizing the fact that there should be very close functional alignments between the concept of traditional signatures and electronic signatures. The Model Law also has recognized the need to implement the functional aspects of traditional signatures into the technical implementation of electronic signatures in order to provide greater security to electronic transactions. However, what is not fully functional is the implementation system. While countries like Australia have recognized the need to move faster in this area and started developing their own framework, which is slightly different from the Model Law, a number of other countries have not yet recognized the concept of electronic signatures. This poses the problem of international harmony in implementing these radically new concepts.

Irrespective of the recent and encouraging developments in the area of electronic signatures, it is concluded that more concentrated effort is needed to arrive at perfection in implementing the centuries old traditional signature system. While such a system is slowly emerging the following three points must be remembered for future refinements:

- The capability of electronic signatures being removed without trace should be remedied.

- A trusted path between the memory, other devices as well as wireless service providers generating electronic signature should be established.

- Software applications should be capable of verifying signatures while devices are in roaming mode in order for third parties to witness and attest electronic documents.

REFERENCE

Clarke, R. (2003). *Identification and Authentication Fundamentals*. Retrieved 10 Feb 2004, 2004

Desai, N. (1999). *Legal and policy framework for e-commerce in India*. Bombay: Nishi Desai Associates.

Evans, S. (2000). Pacing out the last mile. *Australian communications*(February), 81-88.

Judge, P. (1998). Little guys still say NO to the net. *Business Week*, 134.

Kuechler, W., & Grupe, F. H. (2003). Digital Signatures: A Business View. *Information Systems Management*(Winter 2003), 19-28.

Lovell, C. (2000). What constitutes a low impact telecommunications facility. *Australian communications*(February), 53-54.

McCullagh, A., Little, P., & Caelli, W. (1998). Electronic Signatures: Understand the past to develop the future. *University of NSW Law Journal, 21*(2), 1-13.

Sneddon, M. (1998). Legislating to facilitate Electronic Signatures and Records: Exceptions, Standards and the impact on the Statute Book. *University of NSW Law Journal, 21*(2), 1-37.

Stowe, B. (2000). Wireless networking looks attractive, but what about the cost of keeping it secure? *Infoworld*(May), 92.

Wyrough, W., & Klien, R. (1998). The Electronic Signature Act of 1996: Breaking down barriers to widespread electronic commerce in Florida. *Florida State University Law Review, 24*(2), 407-438.